INFORMATION SYSTEM SECURITY

Computer User Security Agreement

As a user of an information system, I _____ will adhere to the following security rules: (Print User Name)

1. I will use USDA computer systems (computers, laptops, PDAs, and networks) only for authorized purposes.
2. If using USDA computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy and supervisor approval, and without interfering with official business.
3. I will not use USDA resources, including electronic mail and Internet/Worldwide Web access, for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of any activities prohibited by law.
4. I will not load any unapproved software (software from home, games, etc) or install hardware such as peripheral devices (external hard drives, docking stations, etc.) on any USDA system. If I need software or hardware loaded on my system, I will obtain written approval from my supervisor and coordinate the installation with my System Administrator or Help Desk (e.g., Service Center Agencies can only load Common Computing Environment hardware/software certified by the OCIO-ITS IO Lab).
5. I will not download file-sharing software (including MP3 music and video files), peer-to-peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT system, or network.
6. I will not try to access data or use operating systems or programs, except as specifically authorized.
7. I know I will be issued Government user identifiers (user IDs) and passwords to authenticate my computer account. After receiving them—
    a. If given a password, I will immediately change the password.
    b. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report this issue to my supervisor or to my assigned Information System Security Program Manager (ISSPM), or Information System Security Point of Contact (ISSPOC).
    c. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged onto a system with that account.
    d. I will ensure that my password is changed on a regular basis or if it is compromised, whichever is sooner.
    e. I understand that USDA has a password complexity requirement, and I will use passwords that meet this requirement.
    f. I will not write down my password or store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media unless approved in writing by the USDA Agency Security Staff.

To be filed in Official Personnel Folder (OPF) or Official ISSPOC Folder
OPF Left Side – KEEP ON TOP

8. I will log completely off workstations, or use screen savers that require a password to reactivate the workstation; any time I leave the workstation unattended (except in genuine emergencies, such as fire).
9. I will scan all removable media (for example, disks, CDs, thumb drives) for malicious software (for example, viruses, worms, etc) before using it on any government computer, system, or network.
10. I will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.
11. I will report promptly to my supervisor and/or to my assigned USDA Agency Security Staff any actual or suspected violation of security.
12. I will stay abreast of security issues via education and awareness products distributed throughout USDA—

    - I have completed the Computer Security Awareness (CSAT) and Privacy Basics Training courses and completion will be recorded in the Agriculture Learning (AgLearn) system.

    - I verify that I have read and will abide by the "Security Expectations and Rules of Behavior" brochure available at: ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures

    - I verify that I have read the "Security Incident Response Guide for Users" available at: ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures

    - I verify that I will read and abide by all NRCS Title 270 (Information Resources Management) Electronic Directives System (eDirectives) located via my.NRCS at: https://my.nrcs.usda.gov/management.aspx or at http://directives.sc.egov.usda.gov/

    - I verify that I will reference (when appropriable) the OCIO-Information Technology Services (ITS) Security Policies located at: http://www.ocionet.usda.gov/ocio/its/security/library/security_Library.asp

I know that my actions as a user can greatly affect the security of the system. My signature on this agreement indicates that I understand my responsibilities as a user of government computer systems and that I adhere to regulatory guidance. I am subject to administrative and/or disciplinary action if I violate USDA computer policy.

User:

_____ _____

Signature Date

Supervisor or Office Manager or Contracting Representative:

_____

Printed Name

_____ _____

Signature Date

To be filed in Official Personnel Folder (OPF) or Official ISSPOC Folder
OPF Left Side – KEEP ON TOP